Attorney Docket No. 1572.1150

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Jeom-jin CHANG

Application No.: Unassigned | Group Art Unit: Unassigned

Filed: June 26, 2003 | Examiner: Unassigned

For: METHOD FOR BIOS SECURITY COMPUTER SYSTEM

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Korean Patent Application No. 2002-76598

Filed: December 4, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 6/26/03

By: _____

Michael D. Stein
Registration No. 37,240

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0076598
Application Number PATENT-2002-0076598

출 원 년 월 일 : 2002년 12월 04일
Date of Application DEC 04, 2002

출 원 인 : 삼성전자 주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2002 년 12 월 23 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.12.04
【발명의 명칭】	컴퓨터 시스템의 바이오스 보안 유지방법
【발명의 영문명칭】	Method for BIOS security in computer system
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	허성원
【대리인코드】	9-1998-000615-2
【포괄위임등록번호】	1999-013898-9
【발명자】	
【성명의 국문표기】	장점진
【성명의 영문표기】	CHANG,JEOM JIN
【주민등록번호】	731115-1674618
【우편번호】	442-370
【주소】	경기도 수원시 팔달구 매탄동 주공그린빌 3단지아파트 305동 101호
【국적】	KR
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 허성원 (인)
【수수료】	
【기본출원료】	18 면 29,000 원
【가산출원료】	0 면 0 원
【우선권주장료】	0 건 0 원
【심사청구료】	0 항 0 원
【합계】	29,000 원

【요약서】

【요약】

본 발명은 컴퓨터 시스템의 바이오스 보안유지 방법에 관한 것으로서, 사용자의 패스워드와 바이오스롬의 제품일련번호를 바이트 합산한 체크섬값을 미리 저장하는 단계와; 상기 미리 저장된 체크섬값과, 상기 사용자에 의해 입력되는 패스워드와 상기 바이오스롬의 제품일련번호를 합산하여 산출된 체크섬값을 비교하는 단계와; 상기 미리 저장된 체크섬값과 상기 산출된 체크섬값이 일치하는 경우 상기 바이오스롬의 쓰기를 인에이블하는 단계를 포함하는 것을 특징으로 한다. 이에 의하여 제조자에 의해 부여되는 바이오스롬의 고유한 제품일련번호와 사용자에 의해 설정된 패스워드를 이용하여 컴퓨터 시스템상의 바이오스롬내의 바이오스가 악의적이거나 임의로 변경 또는 소거되는 것을 방지함으로써 바이오스의 보안을 유지할 수 있다.

【대표도】

도 2

【명세서】

【발명의 명칭】

컴퓨터 시스템의 바이오스 보안 유지방법{Method for BIOS security in computer system}

【도면의 간단한 설명】

도 1은, 본 발명에 따른 POST과정 중 바이오스롬의 보안설정을 위한 절차를 나타내는 흐름도,

도 2는, 도 1에 기초하여 시스템 실행 중 바이오스롬의 보안유지를 위한 절차를 나타내는 흐름도,

도 3은, 종래 컴퓨터 시스템의 바이오스롬의 보안유지 구조도이다.

<도면의 주요부분에 대한 부호의 설명>

10 : 중앙처리장치	30 : 사우스브릿지칩
40 : SIO칩	41 : 바이오스쓰기방지핀
50 : 바이오스롬	51 : CS신호 입력부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<8> 본 발명은 컴퓨터 시스템에 관한 것으로서, 보다 상세하게는 컴퓨터 시스템의 바이오스롬에 내장된 바이오스의 보안을 유지할 수 있는 방법에 관한 것이다.

<9> 컴퓨터 시스템에서 바이오스는 CMOS Setup값을 이용하여 POST(Power On Self Test)를 통한 시스템의 초기화와 이상 유무 확인, 또 운영체제 기동후의 실행(Run-time) 기능 등 그 역할이 중대하다.

<10> 도 3은 일반적인 컴퓨터 시스템에서 하드웨어적으로 구현된 바이오스롬의 보안유지 구조를 도시한 것이다. 컴퓨터 시스템에서 비디오 및 메모리를 제어하는 노스브릿지칩(20) 및 다양한 주변기기를 제어하는 사우스브릿지칩(30)은 중앙처리장치(10)와 버스구조로 연결되어 있다. 여기서 바이오스가 저장되는 바이오스롬(50)은 쓰기가능한 플래시롬으로 구성되어 사우스브릿지칩(30)과 LPC(Low Pin Count)버스로 연결되어 있다. 그리고 Legacy Port 및 FDD 등의 입출력제어기인 SIO(Super Input/Output)칩(40)도 사우스브릿지(30)와 LPC버스를 통하여 연결되어 있다.

<11> 바이오스롬(50)에 쓰기방지를 위하여, 범용입출력(General Purpose Input/Output:GPIO)기능을 구비한 칩셋의 GPIO핀 중 한 핀을 바이오스 쓰기방지용(BIOSWP#)핀으로 설정할 수 있다. 도면에서는 SIO칩(40)에 마련된 GPIO핀(41)을 BIOSWP#핀으로 설정하여, 이로부터 바이오스롬(50)의 플래시영역의 입력단(51)을 선택하기 위한 신호(CS신호)가 출력된다. 이 핀에서 출력되는 신호의 하이/로우 여부에 따라 바이오스롬(50)의 플래시영역에 쓰기 동작을 인에이블하거나 디스에이블 하도록 한다. 이러한 바이오스롬의 쓰기동작은 사우스브릿지칩(30)에 마련된 GPIO핀들중 한 핀을 BIOSWP#핀으로 설정하여 이용할 수도 있다.

<12> 따라서 바이오스에 의한 POST를 수행하면서 BIOSWP#핀을 인에이블로 설정하면 바이오스롬의 플래시영역에 대한 소거 또는 쓰기동작을 방지할 수 있다. 아울러 바이로스롬의 ESCD(Extended System Configuration Data)영역을 기록하거나 바이오

스의 업데이트가 필요한 경우에는 불활성메모리관리자(PNP NVRAM manager)를 이용하여 BIOSWP#핀을 디스에이블로 설정하여 바이오스롬의 플래시 영역에 쓰기동작이 가능하다.

<13> 그러나, SIO칩이나 사우스브릿지칩상에서 BIOSWP#핀의 위치가 노출되거나, IO트랩 영역으로 할당된 메모리맵 IO주소와 GPIO핀 설정방법과 같은 제어방법이 노출되는 경우에는 임의로 BIOSWP#핀의 기능을 디스에이블로 설정하여 바이오스롬의 내용을 변경 또는 삭제할 수 있다는 보안상의 문제점이 존재한다. 따라서 컴퓨터 시스템에서 바이오스에 대한 보안체계의 허술로 악성 바이러스에 의한 바이오스 변경시 시스템의 부팅이 불가능하거나 기능이 제대로 작동하지 않는 등 컴퓨터 시스템의 치명적인 손상을 초래할 수 있다. 실제로 체르노빌 바이러스(CIH바이러스)는 바이오스롬의 내용을 삭제시켜 사용자들에게 심각한 피해를 입힌 사례도 있다.

【발명이 이루고자 하는 기술적 과제】

<14> 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 컴퓨터 시스템에서 바이오스롬의 내용을 변경하고자 할 경우에는, 제조자에 의해 부여되는 제품의 고유 특징인 일련번호와 사용자에 의해 부여되어지는 감독자 패스워드를 이용하여 바이오스가 악의적이거나 임의로 변경 또는 소거되는 것을 방지하여 바이오스의 보안을 유지할 수 있는 방법을 제공하고자 한다.

【발명의 구성 및 작용】

<15> 상기 목적은, 사용자의 패스워드와 바이오스롬의 제품일련번호를 바이트 합산한 체크섬값을 미리 저장하는 단계와, 상기 미리 저장된 체크섬값과, 상기 사용

자에 의해 입력되는 패스워드와 상기 바이오스롬의 제품일련번호를 합산하여 산출된 체크섬값을 비교하는 단계와, 상기 미리 저장된 체크섬값과 상기 산출된 체크섬값이 일치하는 경우 상기 바이오스롬의 쓰기를 인에이블하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법에 의하여 달성된다.

<16> 여기서, 상기 체크섬값을 미리 저장하는 단계는, POST수행시 사용자의 패스워드가 설정되었는지 여부를 판단하는 단계와; 상기 패스워드가 설정된 경우 상기 바이오스롬의 제품일련번호를 판단하는 단계와; 상기 제품일련번호가 제조상의 디폴트값이 아닌 경우, 상기 패스워드와 상기 제품일련번호를 바이트 합산하여 상기 체크섬값을 기억장소에 저장하는 단계를 포함하는 것이 바람직하다.

<17> 그리고, GPIO기능을 구비한 칩셋의 바이오스 쓰기방지 영역으로 할당된 메모리맵 입출력영역을 입출력트랩 영역으로 설정하여 입출력트랩을 인에이블하는 단계를 더 포함하는 것이 바람직하다.

<18> 또한, 상기 합산된 체크섬값을 기억장소에 저장하는 단계는, 상기 합산된 체크섬값을 CMOS램 또는 불활성메모리(PNP NVRAM)에 저장하는 단계인 것이 바람직하다.

<19> 한편, 상기 체크섬값을 비교하는 단계 앞에, GPIO기능을 구비한 칩셋의 바이오스 쓰기방지 영역으로 할당된 메모리맵 입출력영역을 입출력트랩 영역으로 설정하여 입출력트랩을 인에이블하는 단계와; 상기 시스템의 실행 도중 상기 바이오스쓰기방지를 디스에이블하는 이벤트가 발생하는 단계와; 상기 입출력트랩을 디스에이블로 설정하는 단계와; 상기 바이오스롬의 제품일련번호를 판단하는 단계와; 상기 제품일련번호가 제조상의 디폴트값이 아닌 경우, 상기 사용자가 패스워드를 입력하는 단계와; 상기 패스워드와 상기 제품일련번호를 합산하여 체크섬값을 산출하는 단계를 더 포함하는 것이 바람직하다.

<20> 여기서 상기 바이오스롬의 쓰기를 인에이블한 뒤 상기 입출력트랩을 인에이블하는 단계를 더 포함하도록 하는 것이 바람직하다.

<21> 그리고 상기 제품일련번호가 제조공정상의 디폴트값이거나, 상기 체크섬값이 일치하지 않는 경우에 에러메세지를 표시하는 단계를 더 포함하는 것이 바람직하다.

<22> 또한, 상기 바이오스 쓰기방지를 디스에이블하는 이벤트가 발생하는 단계는, 상기 입출력트랩이 발생하거나, 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생하는 단계인 것이 바람직하다.

<23> 아울러, 상기 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생한 경우, 상기 입출력트랩이 인에이블로 설정되었는지를 판단하는 단계를 더 포함하는 것이 바람직하다.

<24> 한편, 상기 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생한 때에 상기 입출력트랩이 인에이블로 설정되어 있지 아니한 것으로 판단되는 경우 에러메세지를 표시하는 단계를 더 포함하는 것이 바람직하다.

<25> 그리고, 상기 에러메세지를 표시한 뒤 상기 입출력트랩을 인에이블하는 단계를 더 포함하는 것이 바람직하다.

<26> 이하에서는 첨부 도면을 참조하여 본 발명에 대하여 상세히 설명한다.

<27> 본 발명에서는 도 3에 나타난 바와 같은 컴퓨터 시스템에서 바이오스롬의 보안유지 구조를 하드웨어적으로 변경하지 않으면서, 바이오스롬내의 데이터를 효과적으로 보호할 수 있는 방법을 제공한다. 즉 본 발명에서는 POST과정에서 사용자가 설정한 감독자패스워드와 바이오스롬의 ESCD영역에서 읽어낸 소정의 제품일련번호를 바이트 합산한 체크섬

값을 CMOS램(미도시) 또는 불활성메모리(PNP NVRAM) 영역의 기억장소에 미리 저장해 두고, 시스템 실행시에 바이오스롬(50)의 플래시영역에 외부로부터 쓰기동작을 시도할 경우에는, 사용자가 입력하는 패스워드와 및 제품일련번호로부터 산출된 체크섬값과 미리 저장된 체크섬값을 비교하는 과정을 거치도록 한다. 이에 따라 비교되는 두 체크섬값이 일치할 경우에, 사우스브릿지칩(30)이나 SIO칩(40)에 마련된 BIOSWP#핀을 디스에이블시키고, 그에 따라 바이오스롬(50)의 플래시영역의 입력핀(51)에 쓰기허용신호(CS신호)가 인가되어 바이오스롬의 플래시영역에 대한 소거 또는 쓰기동작을 가능하도록 한다.

<28> 도 1은 본 발명에 따른 컴퓨터 시스템의 POST과정 중 바이오스롬의 보안절차를 설정하기 위한 과정을 나타내는 흐름도이다. 도시된 바와 같이 바이오스에 의한 POST과정을 거치면서 사용자에 의해 패스워드가 설정되었는지 여부를 판단한다(S10). 패스워드는 사용자가 CMOS설정 과정에서 미리 설정할 수 있다. 또한 위 판단과정에서 패스워드가 설정되지 않은 경우에는 사용자의 선택에 따라 패스워드를 다시 설정하도록 하거나, 보안절차의 설정과정을 생략하도록 할 수도 있다. 사용자 패스워드가 설정되어 있는 경우에는, 바이오스롬(50)의 ESCD영역에서 읽어낸 제품일련번호가 제조공정상의 디폴트값인지 여부를 확인한다(S11). 바이오스롬(50)이 정상적인 출하과정을 통하여 출시된 제품인 경우에는 제조공정상의 디폴트값이 아닌 소정의 제품일련번호를 확인할 수 있다. 그리고 정상적인 출하과정을 통하여 출시된 제품이 아닌 경우에는 제품일련번호가 디폴트값을 갖고 있으므로 바이오스롬을 보호하기 위하여 보안절차의 설정과정을 생략하도록 할 수도 있다.

<29> 만약 바이오스롬(50)이 디폴트값이 아닌 소정의 제품일련번호를 갖고 있어서 정상적인 출하제품임이 확인되면, 사용자에 의해 설정된 감독자 패스워드와 제품일련번호를

바이트 합산한 체크섬값을 소정의 기억장소에 저장하도록 한다(S12, S13). 이때 체크섬값의 기억장소는 CMOS램 또는 불활성메모리(NVRAM) 영역에 저장하도록 하는 것이 바람직하다. 이에 따라서 SIO칩(40) 또는 사우스브릿지칩(30)과 같이 GPIO기능을 구비한 칩셋에서 BIOSWP#핀 영역에 해당하는 메모리맵된 입출력영역(IO영역)을 입출력트랩(IO Trap) 영역으로 설정하여 IO트랩을 인에이블로 설정하도록 한다.

<30> 이와 같이 사용자 패스워드와 바이오스롬의 제품일련번호에 기초한 체크섬값을 미리 저장하도록 함으로써 바이오스롬의 보안설정을 위한 절차를 종료한다.

<31> 도 2는 시스템 실행시 바이오스롬(50)으로 바이오스쓰기방지를 디스에이블하기 위한 이벤트가 발생되었을 경우의 처리 절차를 나타낸다.

<32> 시스템의 실행중에 바이오스롬(50)의 바이오스쓰기방지을 디스에이블하기 위하여 불활성메모리관리자(PNP NVRAM manager)를 통하여 롬바이오스 영역을 변경하려고 할 경우(S20)나, BIOSWP#핀(41)에 해당하는 메모리맵된 입출력영역을 접근하여 IO트랩이 발생되어 IO트랩처리기를 통하여 처리되는 경우(S22)에는 다음과 같은 절차를 거쳐 보안을 유지한다.

<33> 먼저 불활성메모리관리자(PNP NVRAM manager)를 통하여 롬바이오스 영역을 변경하고자 할 때에는, IO트랩이 인에이블되었는지 여부를 판단한다(S21). 이때 IO트랩이 인에이블되어 있지 아니한 것으로 확인되면, 에러메세지를 표시하고(S29) IO트랩을 다시 인에이블하도록 할 수 있다(S28). 그리고 S21에서 IO트랩이 인에이블되어 있음을 확인하거나, IO트랩처리기에 의해 IO트랩 발생을 확인한 경우(S22)에는 추가적으로 SMI(System Management Interrupt)가 발생되는 것을 방지하기 위하여 IO트랩을 디스에이블시킨다(S23).

<34> 그 다음에 바이오스롬(50)이 정상적인 출하제품인지를 판단하기 위하여 제품일련번호를 확인한다(S24). 만약 제품일련번호가 생산공정에서의 디폴트값인 경우에는 정상적인 출하제품이 아니므로, 롬바이오스를 보호하기 위하여 에러메세지를 출력하여(S29) BIOSWP#핀(41)을 디스에이블 시키지 않는다. 그러나 제품일련번호가 생산공정에서의 디폴트값이 아닌 경우에는 정상적인 출하제품이므로, 패스워드 입력창을 표시하여 사용자가 감독자패스워드를 입력하도록 한다(S25).

<35> 이에 따라 입력된 감독자패스워드와 제품일련번호를 바이트 합산하여 체크섬값을 산출한다(S25). 산출된 체크섬값과 POST과정에서 미리 저장된 체크섬값을 비교하여(S26), 서로 일치하는 경우에는 BIOSWP#핀(41)을 디스에이블 상태로 설정하여(S27), 바이오스롬(50)의 플래시영역으로 접근이 가능하도록 한다. 그러나, 패스워드가 잘못 입력되는 등으로 인하여, 산출된 체크섬값이 미리 저장된 체크섬값과 일치하지 않는 경우에는 에러 메시지를 출력하고(S29) 롬바이오스 영역을 보호하기 위하여 BIOSWP#핀(41)을 인에이블 상태로 유지하도록 한다. 이에 따라 바이오스롬(50)내에 시스템 설정에 필요한 데이터를 기록할 수 있는 상태가 된다. 위와 같은 과정을 거친 후 다시 사우스브릿지칩(30)이나 SIO칩(40)에서 BIOSWP#핀 영역에 해당하는 메모리맵으로 할당된 IO영역의 IO트랩을 인에이블시켜(S28), 추가적인 SMI의 발생에 대비하도록 한다.

<36> 이와 같이, 본 발명의 바이오스 보안유지 방법에 따르면, 시스템의 실행 중, 임의로 바이오스쓰기방지핀을 디스에이블하기 위하여 바이오스쓰기방지핀에 해당하는 할당된 메모리맵 IO영역을 접근하거나, 불활성메모리 관리자 등을 통하여 롬바이오스 영역을 변경하려고 할 경우, 제품일련번호와 사용자 패스워드의 합산값인 체크섬값이 미리 저장된 값과 일치할 때에만 바이로스롬으로의 접근이 가능하도록 하여 바이오스쓰기방지핀을

디스에이블시킬 수 있다. 만약 두 체크섬값이 일치하지 않는 경우에는 바이오스쓰기방지핀의 디스에이블 설정이 불가능하므로 바이오스롬을 보호할 수 있게 된다.

<37> 따라서, 본 발명의 구성에 의해, GPIO기능을 구비한 SIO칩이나 사우스브릿지칩에서 BIOSWP#핀의 위치, 메모리맵된 IO주소와 GPIO핀 설정방법 등의 제어방법이 노출되는 경우에도, 바이오스롬의 내용을 임의로 변경 또는 삭제하는 행위를 방지할 수 있다. 또한 아울러 바이로스롬의 ESCD(Extended System Configuration Data)영역을 기록하거나 바이오스의 업데이트가 필요한 경우에도 불활성메모리관리자(PNP NVRAM manager)를 이용하여 BIOSWP#핀을 디스에이블로 설정하여 바이오스롬의 플래시 영역에 쓰기동작이 가능하다. 이에 따라 컴퓨터 시스템에서 바이오스에 대한 보안체계를 강화함으로서 체르노빌 바이러스 등의 악성 바이러스 에 의한 바이오스 침입시 시스템의 부팅이 불가능하거나 기능이 제대로 작동하지 않는 등 컴퓨터 시스템의 치명적인 손상을 방지할 수 있게 된다. 아울러 바이로스롬의 성능개선을 위한 업데이트도 안전하게 수행할 수 있게 된다.

<38> 이와 같이 본 발명은 사우스브리지칩 또는 SIO칩의 GPIO핀중 한 핀으로 BIOSWP#로 이용하여 바이오스롬을 보호하는 하드웨어 구조를 이용한 것이다. 여기에 제조자에 의해 부여되는 제품일련번호와 사용자에 의해 부여되는 감독자 패스워드를 확인하는 기능을 부가함으로서 바이오스롬의 임의적인 또는 악의적인 위조, 변경 또는 소거 동작에 대하여 효과적으로 방지할 수 있다.

【발명의 효과】

<39> 상기와 같이 본 발명에 따르면, 제조자에 의해 부여되는 바이오스롬의 고유한 제품일련번호와 사용자에 의해 설정된 패스워드를 이용하여 컴퓨터 시스템상의 바이오스롬내

의 바이오스가 악의적이거나 임의로 변경 또는 소거되는 것을 방지함으로써 바이오스의 보안을 유지할 수 있다.

【특허청구범위】

【청구항 1】

사용자의 패스워드와 바이오스롬의 제품일련번호를 바이트 합산한 체크섬값을 미리 저장하는 단계와,

상기 미리 저장된 체크섬값과, 상기 사용자에 의해 입력되는 패스워드와 상기 바이오스롬의 제품일련번호를 합산하여 산출된 체크섬값을 비교하는 단계와,

상기 미리 저장된 체크섬값과 상기 산출된 체크섬값이 일치하는 경우 상기 바이오스롬의 쓰기를 인에이블하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법

【청구항 2】

제1항에 있어서,

상기 체크섬값을 미리 저장하는 단계는,

POST수행시 사용자의 패스워드가 설정되었는지 여부를 판단하는 단계와,

상기 패스워드가 설정된 경우 상기 바이오스롬의 제품일련번호를 판단하는 단계와,

상기 제품일련번호가 제조상의 초기값이 아닌 경우, 상기 패스워드와 상기 제품일련번호를 바이트 합산하여 상기 체크섬값을 기억장소에 저장하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 3】

제2항에 있어서,

GPIO기능을 구비한 칩셋의 바이오스 쓰기방지 영역으로 할당된 메모리맵 입출력영역을 입출력트랩 영역으로 설정하여 상기 입출력트랩을 인에이블하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 4】

제2항에 있어서,

상기 합산된 체크섬값을 기억장소에 저장하는 단계는, 상기 합산된 체크섬값을 CMOS램 또는 불활성메모리(PNP NVRAM)에 저장하는 단계인 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 5】

제1항에 있어서,

상기 체크섬값을 비교하는 단계 앞에,

GPIO기능을 구비한 칩셋의 바이오스 쓰기방지 영역으로 할당된 메모리맵 입출력영역을 입출력트랩 영역으로 설정하여 상기 입출력트랩을 인에이블하는 단계와,

상기 시스템의 실행 도중 상기 바이오스쓰기방지를 디스에이블하는 이벤트가 발생하는 단계와,

상기 입출력트랩을 디스에이블로 설정하는 단계와,

상기 바이오스롬의 제품일련번호를 판단하는 단계와,

상기 제품일련번호가 제조상의 디폴트값이 아닌 경우, 상기 사용자가 패스워드를 입력하는 단계와,

상기 패스워드와 상기 제품일련번호를 합산하여 체크섬값을 산출하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 6】

제5항에 있어서,

상기 바이오스롬의 쓰기를 인에이블한 뒤 상기 입출력트랩을 인에이블하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 7】

제5항에 있어서,

상기 제품일련번호가 제조공정상의 디폴트값이거나, 상기 체크섬값이 일치하지 않는 경우에 에러메세지를 표시하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 8】

제5항에 있어서,

상기 상기 바이오스쓰기방지를 디스에이블하는 이벤트가 발생하는 단계는, 상기 입출력트랩이 발생하거나, 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생하는 단계인 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 9】

제8항에 있어서,

상기 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생한 경우, 상기 입출력트랩이 인에이블로 설정되었는지를 판단하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【청구항 10】

제9항에 있어서,

상기 불활성메모리관리자에 의해 상기 바이오스롬의 쓰기 동작이 발생한 때에 상기 입출력트랩이 인에이블로 설정되어 있지 아니한 것으로 판단되는 경우 에러메세지를 표시하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

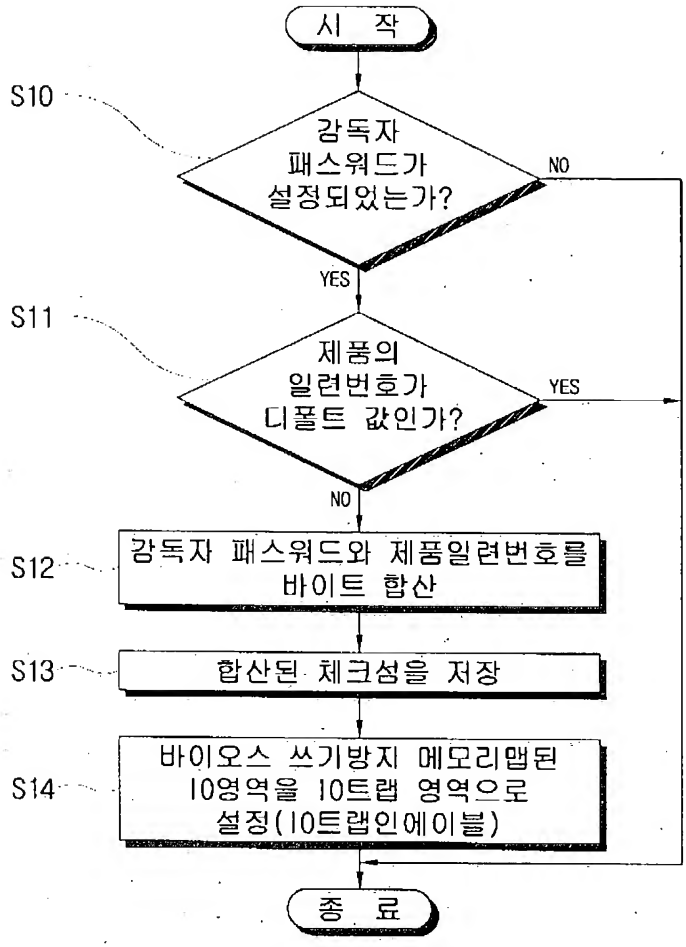
【청구항 11】

제7항 또는 제10항에 있어서,

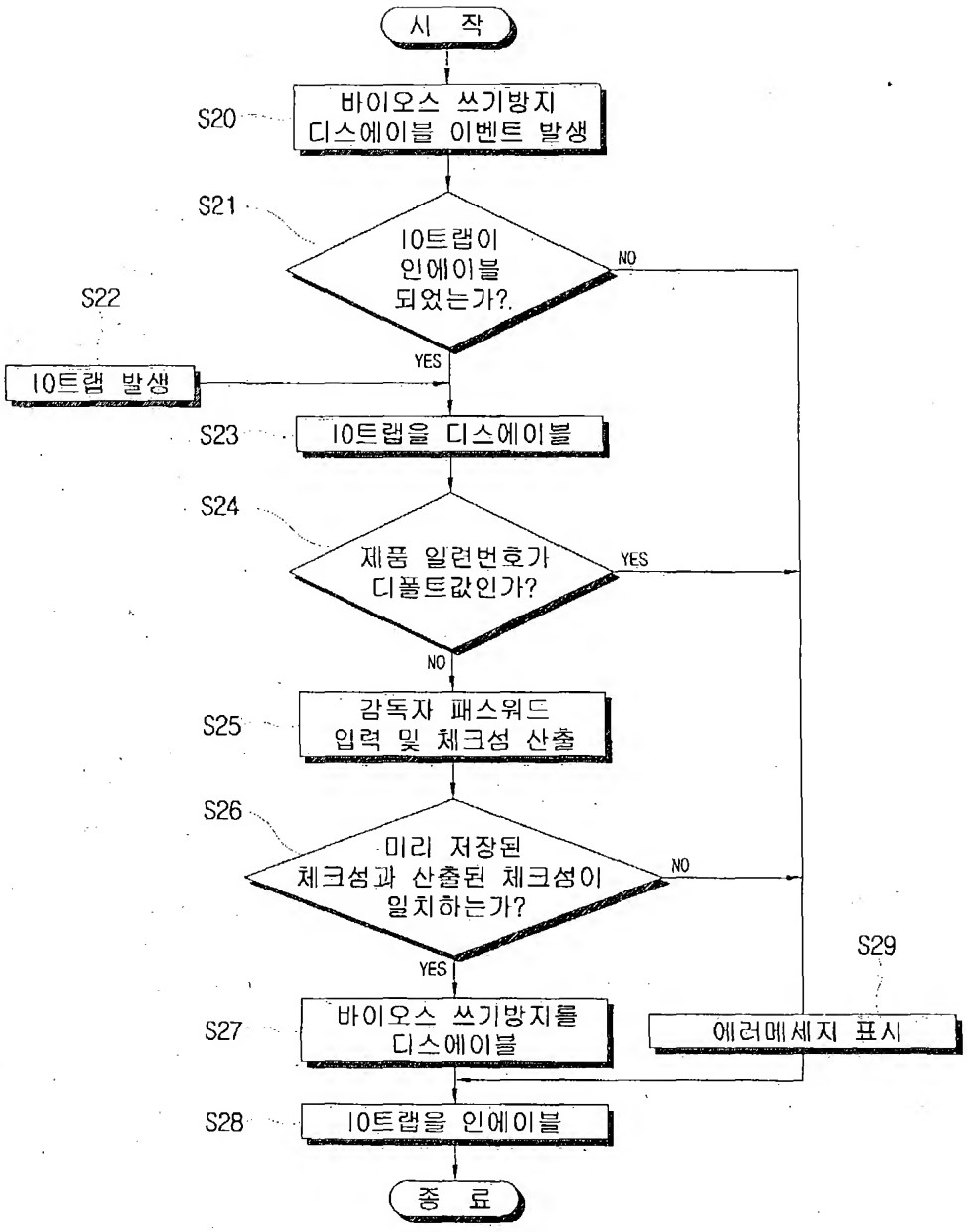
상기 에러메세지를 표시한 뒤 상기 입출력트랩을 인에이블하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 시스템의 바이오스 보안유지 방법.

【도면】

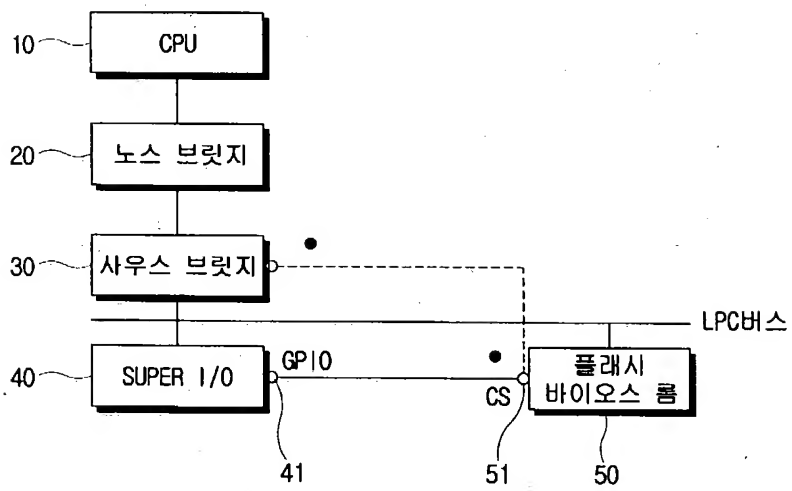
【도 1】


시 작
S10
감독자 패스워드가 설정되었는가?
NO
YES
S11
제품의 일련번호가 디폴트 값인가?
YES
NO
S12
감독자 패스워드와 제품일련번호를 바이트 합산
S13
합산된 체크섬을 저장
S14
바이오스 쓰기방지 메모리맵된 IO영역을 IO트랩 영역으로 설정(IO트랩인에이블)
종 료

【도 2】


시 작
S20
바이오스 쓰기방지 디스에이블 이벤트 발생
S21
IO트랩이 인에이블 되었는가?
NO
S22
YES
IO트랩 발생
S23
IO트랩을 디스에이블
S24
제품 일련번호가 디폴트값인가?
YES
NO
S25
감독자 패스워드 입력 및 체크섬 산출
S26
미리 저장된 체크섬과 산출된 체크섬이 일치하는가?
NO
YES
S29
S27
바이오스 쓰기방지를 디스에이블
에러메세지 표시
S28
IO트랩을 인에이블
종 료

【도 3】


10
CPU
20
노스 브릿지
30
사우스 브릿지
LPC버스
40
SUPER I/O
GPIO
CS
플래시
바이오스 롬
41
51
50